Domande LAS

Introduzione al corso

1. **Le certificazioni professionali in ambito Linux sono utili sul mercato del lavoro. V**
2. **L'amministratore di sistema non ha responsabilità legali, solo operative. F**
3. **È consigliabile che l'amministratore effettui il login come root, in quanto la maggior parte delle attività richiedono i privilegi corrispondenti. F**
   Eseguire operazioni come root può mettere a repentaglio la salute del sistema, e va quindi fatto con cautela solo quando è necessario.

Shell scripting

4. **Gli alias di bash possono contenere altri alias, che vengono espansi. V**
   Il secondo passo della Shell expansion è proprio il controllo del primo token, se è un alias o meno. Se lo è lo espande e riparte dal primo punto, permettendo alias ricorsivi. Uno stesso alias però non verrà mai espanso due volte.
5. **Gli alias di bash possono espandere ricorsivamente se stessi. F**
   Il secondo passo della Shell expansion è proprio il controllo del primo token, se è un alias o meno. Se lo è lo espande e riparte dal primo punto, permettendo alias ricorsivi. Uno stesso alias però non verrà mai espanso due volte.
6. **Le pagine di manuale sono divise in sezioni. V**
   Le sezioni possono indicare parametri specifici per input, output, o altre informazioni utili.
7. **Non possono esistere due man page con lo stesso nome. F**
   Queste sono tuttavia identificate grazie a un numero, che permette di identificare le pagine in modo univoco
8. **Un comando invocato col nome "nudo" del programma (esempio: ls) viene eseguito da bash di default se trovato nella directory corrente. F**
   (UPDATE: Un comando invocato col nome del programma privo di percorso (esempio:ls) viene eseguito se trovato nella directory corrente)
   I comandi senza path si possono chiamare solo se la loro directory è collocata nella variabile d'ambiente PATH.

Device filesystem

9. **I device driver rispettano le interfacce delle system call standard (open, close, read, ...) e implementano i comandi corretti per il corrispondente dispositivo. V**

   Quando viene caricato un modulo questo dichiara che slot nella tabella dei puntatori vuole occupare, registrando nelle celle i puntatori alle proprie implementazioni delle system call.

10. **I file in /dev contengono una copia dei dati dei rispettivi dispositivi. F**

    In /dev si trovano file speciali che funzionano come punti di accesso alle periferiche, e sono astratti. Su di essi vengono invocate le operazioni definite nei device driver.

11. **Un disco può essere formattato senza essere partizionato. V**

    La partizione di un disco è la suddivisione di esso in un sottoinsieme di blocchi, ciascuno dei quali si presenta come dispositivo indipendente. La formattazione crea il filesystem in una partizione. Non è necessario che un disco sia partizionato per essere formattato.

12. **Un disco e una sua partizione sono entrambi dispositivi a blocchi. V**

    Un disco è un dispositivo a blocchi. Le partizioni sono sottoinsiemi di blocchi del disco. Dunque sono entrambi dispositivi a blocchi.

13. **I file di un filesystem possono essere acceduti direttamente con la notazione /dev/partizione/percorso/file. F**

    La formattazione crea il filesystem in una partizione, e permette l'accesso ai file mediante il modello del Virtual File System, che astrae dall'organizzazione dei dati. Tramite l'operazione di mount, il partizionamento crea una gerarchia locale di directory, che viene innestata nella gerarchia globale in modo trasparente.

14. **I file in /dev corrispondono uno-a-uno coi device installati sul sistema. F**

    I file in /dev sono punti di accesso alle periferiche astratti. Le entry della tabella dei puntatori corrispondono uno-a-uno coi device installati.

Gestione servizi

15. **I log non possono essere analizzati in tempo reale. F**

    I log sono normalissimi file di testo e in quanto tali possono essere analizzati in tempo reale.

16. **I target di systemd sono grosso modo equivalenti ai runlevel di SysVinit. V**

    Systemd rimpiazza i runlevel di Sysvinit con i target. I target sono 6 più uno di emergenza.

17. **Il carico riportato da uptime rappresenta la percentuale di utilizzo della CPU. F**

Uptime indica il tempo dall'avvio del sistema, gli utenti connessi e il carico medio degli ultimi minuti. Il comando top invece riassume ps, uptime, free e dà un'indicazione dettagliata sull'uso della CPU.

18. ***df* e *du* sono strumenti differenti per ottenere la stessa informazione. F**
    df mostra l'utiizzo dello spazio sul disco, mentre du permette di calcolare lo spazio occupato dai file in una directory.
19. **Il selettore local1.info cattura anche messaggi con etichette diverse. V**
    Il selettore local1 è una facility di syslog, mentre info è una priority. Queste direttive sono contenute all'interno del file /etc/syslog.conf. Dal momento che la priority non è preceduta da =, fa match con tutti i messaggi di tale priority e superiori.
20. **La direttiva WantedBy nella definizione di una unit di servizio agisce quando il servizio viene avviato. F**
    La direttiva WantedBy crea automaticamente entry Requires/Wants nelle unit elencate quando questa viene installata.
21. **La pianificazione di attività con cron è riservata all'utente root. F**
    Ogni utente dispone della propria cron table, che può modificare liberamente.
22. **La pianificazione di attività con cron ha un periodo minimo di un minuto. V**
    I periodi possibili sono minito, ora, giorno mese, mese, giorno settimana.
23. **L'azione disable di systemctl impedisce completamente l'avvio del servizio. F**
    Disable lascia la possibilità di usare manualmente start. Mask invece neutralizza l'intera definizio della unit, impedendone il controllo manuale.
24. **Le azioni start e stop di systemctl agiscono istantaneamente sul servizio. V**
    A differenza di enable e disable, start e stop hanno effetto immediato.
25. **Le facility di syslog sono un insieme non ordinato. V**
    Tutte le regole vengono parsate, quindi un messaggio può finire su più destinazioni. Di conseguenza l'ordine non conta.
26. **Se uptime riporta 0.70 0.35 0.88 come valori medi del carico, ciò indica un picco di carico avvenuto di recente e superato. F**
    L'ordine del carico di uptime è 1', 5', 15'. Di conseguenza il carico specificato ha un picco negativo di carico avvenuto di recente e superato.
27. **top è comando più adatto per catturare una "fotografia istantanea" dello stato dei processi in formato flessibile per successive elaborazioni. F**
    L'output di top non si presta particolarmente a elaborazioni, data la sua struttura dinamica. Dal momento che top riassume ps, uptime e free, è consigliabile utilizzare

uno di questi comandi. Per analisi più approfondite sono invece disponibili vmstat e iostat.

28. **Un processo può essere avviato in tre modi: lancio da parte di un utente, avvio al boot da parte di systemd, esecuzione periodica attraverso cron. F**

    Un processo può essere avviato anche con il comando at.

29. **Un servizio di tipo *oneshot* di systemd può risultare attivo anche se non corrisponde ad alcun processo in esecuzione. V**

    I servizi oneshot sono utili quando uno script va lanciato una volta sola per poi uscire. Grazie al setting RemainAfterExit=yes systemd considera il servizio attivo anche dopo l'uscita.

30. **Uno dei vantaggi di utilizzare un sistema di logging centralizzato è la marcatura temporale coerente dei messaggi. V**

    Questo perché macchine diverse possono non essere coerenti tra loro nell'orario, dunque nel timestamping.

31. **top riassume in una schermata l'output di free, ps, uptime. V**

32. ***syslog* classifica i messaggi principalmente sulla base del contenuto. F**

    Syslog classifica i messaggi basandosi sulla loro etichetta, che è composta da facility e priorità.

33. ***lsof* permette, in certe condizioni, di individuare file cancellati. V**

    Lsof lista i file aperti. Se un file è stato cancellato (unlink) dopo l'apertura sarà irreperibile sul filesystem ma referenziato dal processo, quindi visibile a lsof.

34. **La CPU troppo lenta può non essere la causa principale di accodamento di processi e conseguente aumento del carico. V**

    Questo può dipendere non solo dalla velocità della CPU, ma anche dal numero di processori disponibili. (?)

35. **Un task pianificato con cron come 10 22 2,20 * 4 viene eseguito almeno 6 volte al mese. F**

    Questo task viene eseguito tutti i 2 e 20 del mese, inoltre viene eseguito tutti i giovedì del mese alle 22:10. Questo vuol dire che viene eseguito 6 volte al mese solo nei casi in cui né il 2 né il 20 sono giovedì. (Bella domanda ambigua del cazzo)

36. **Il sistema di logging integrato in systemd è avviato prima di syslogd. ?**

    Direi che è vera, perché il journal di systemd è avviato al boot.

Utenti e file

37. **Il comando sudo permette di differenziare quali comandi un utente può eseguire coi privilegi di un altro utente. F**

    Il comando sudo inizialmente permetteva di eseguire un comando solo come superuser. Le versioni più recenti invece permettono di eseguire comandi come altri utenti, secondo le indicazioni presenti nel file /etc/sudoers.

38. **La possibilità di cancellare un file è determinata unicamente dai permessi assegnati alla directory che lo contiene. V**

    In UNIX le directory sono file, e in quanto tali presentano 12 bit di permessi, per quanto questi abbiano un significato leggermente diverso dai file normali. In particolare il permesso R permette di elencare i file all'interno della directory, il permesso W di aggiungere, rimuovere o rinominare un file all'interno della directory, il permesso X di eseguire il lookup dell'i-node della directory.

39. **Ogni file ha come unico proprietario un utente. F**

    Un file ha come proprietari sia un utente che un gruppo

40. **Il comando sudo richiede all'utente la password di root per autorizzare l'esecuzione privilegiata di comandi. F**

    Il comando sudo chiede all'utente la sua password.

41. **Senza permesso di lettura su di una directory, non si possono utilizzare i file in essa contenuti. F**

Alta disponibilità

42. **Il vantaggio dei sistemi NAS su quelli SAN è che non richiedono coordinazione tra i client. V**

    A differenza di SAN, che richiede cooperazione tra utenti, i sistemi NAS non richiedono cooperazione tra gli utenti, dal momento che i dettagli del filesystem sono totalmente trasparenti ai client.

43. **Nell'architettura LVM, un Logical Volume viene costruito in modo da presentare un elenco di blocchi contigui anche se fisicamente utilizza blocchi sparsi. V**

    I Logical Volume dell'architettura LVM estendono il concetto di partizione standard: permette di raggruppare diversi Physical Volume che appaiono contigui anche se sono in realtà sparsi.

44. **Nell'architettura LVM, un Physical Volume viene utilizzato analogamente a una tradizionale partizione di un disco. F**

Un Physical Volume in LVM è l'astrazione di un disco fisso o di una partizione, sono i block device inizializzati con metadati in un apposito settore.

45. **Ripristinare l'integrità di un RAID dopo la sostituzione di un disco può richiedere vari giorni. V**

Le attuali dimensioni dei dischi fanno sì che il ripristino dell'integrità possa durare decine di ore.

46. **Una disponibilità a "6 nove" è facilmente ottenibile con una coppia di computer configurati con heartbeat per il failover automatic. F**

Heartbeat è un sistema di segnalazione della vitalità, e permette di rilevare la necessità di sostituire una risorsa. Ciononostante, non è sufficiente per capire se il sistema è erogato correttamente. Con le architetture cluster non è possibile garantire i five nines.

47. **Un sistema di storage ideale (totalmente resistente a qualsiasi guasto hardware) rende superfluo fare backup. F**

Il backup non serve solo a prevenire guasti hardware ma anche furti e incidenti fisici, quali incendi e simili.

48. **Il downtime riconducibile a problemi software è superiore a quello imputabile a guasti hardware. V**

49. **Tutti i livelli RAID da 0 a 6 aumentano la tolleranza ai guasti. F**

Il sistema che più tutela da guasti RAID1, che richiede che tutti i dischi si rompano contemporaneamente per perdere tutti i dati.

50. **I sistemi NAS sono più efficienti dei sistemi SAN. F**

Nei sistemi SAN i dati sono conservati allo stato grezzo e i blocchi vengono erogati grazie a un protocollo C/S molto leggero che garantisce alta efficienza.

Gestione dei pacchetti software

51. ***yum* e *apt* sono strumenti per la gestione dei pacchetti Debian (e distribuzioni derivate). F**

Yum è uno strumento per la gestione dei pacchetti Red Hat.

52. **Solo il produttore di una distribuzione può realizzare pacchetti installabili correttamente su di un sistema che l'abbia adottata. F**

53. ***dpkg* risolve automaticamente le dipendenze in fase di installazione di un pacchetto. V**

54. **Una distribuzione LTS differisce da una standard per la durata del supporto offerto dal produttore. V**
55. **L'installazione manuale da sorgenti è più flessibile rispetto all'installazione da binari precompilati. V**

Networking di base

56. **Gli indirizzi nel range 169.254.1.0 – 169.254.254.255 sono riservati all'allocazione automatica link local. V**

    Gli indirizzi link local IPv4 vengono assegnati solo se l'interfaccia non ha già un indirizzo assegnato staticamente o con DHCP. Viene scelto un IP random nel range 169.245.1.0 – 169.254.255.255 usando un seme basato sul MAC.
57. **La configurazione di un'interfaccia col comando ip a add 10.1.1.5/24 dev eth1 assegna un indirizzo in modo persistente. F**

    Il comando ip non modifica il file di configurazione ma ha effetto solo a runtime.
58. **L'assegnamento di un indirizzo IPv4 link local avviene prima di interrogare server che potrebbero assegnare un indirizzo diverso all'host. F**

    Un indirizzo IPv4 link local viene assegnato solo se non è stato assegnato un indirizzo statico o con un server DHCP.
59. **L'assegnamento di un indirizzo IPv6 link local secondo il modello SLAAC avviene prima di interrogare server che potrebbero assegnare un indirizzo diverso all'host. V**

    Con SLAAC prima viene generato un indirizzo, o in modo random o usando il MAC. Solo dopo viene verificato se tale indirizzo è già utilizzato, e nel caso cambiato.
60. **NSS (Name Service Switch) è il sistema per la risoluzione dei nomi host in indirizzi IP. F**

    NSS è un sistema per uniformare una grande varietà di database di configurazione e di meccanismi di risoluzione dei nomi.
61. **Gli standard promossi dallo *Zeroconf Working Group* permettono di configurare automaticamente i protocolli da usare a tutti i livelli, da quello fisico a quello applicativo. F**

    Zeroconf non considera la standardizzazione delle comunicazioni a livello applicatico con periferiche, ma i layer comuni a tutti.
62. **Il comando ss non è in grado di riportare alcuna informazione sul traffico che fluisce attraverso un router. V**

    Il comando ss verifica solo lo stato delle connessioni.

63. **Il comando *tcpdump* non permette di rilevare se un processo è in ascolto su di una porta TCP. V**

    Tcpdump intercetta il contenuto dei pacchetti, ma non i processi a cui sono legati.

64. **Il comando ip a add 10.1.1.5/24 dev eth1 modifica anche la tabella di instradamanto del sistema. V**

    Il comando ip sostituisce ifconfig e route.

65. **I nomi assegnati nel dominio .local sono tipicamente strutturati in modo gerarchico secondo le esigenze dell'organizzazione aziendale. F**

    I nomi assegnati nel dominio .local vengono assegnati casualmente basandosi sul MAC del dispositivo.

66. **dnsmasq può essere lanciato in più istanze per servire richieste su interfacce diverse con configurazioni incompatibili tra loro. V**

    L'opzione bind-interfaces evita conflitti qualora si usassera più istanze di dnsmasq per diverse reti connesse al server.

67. **NTP consente la sincronizzazione via Internet con errori ben inferiori al secondo. V**

    NTP è estremamente preciso, permette su WAN uno scarto di poche decine di millisecondi, minore di un millisecondo invece su LAN.

Monitoraggio centralizzato

68. **Attraverso le definizioni SMI, è possibile definire strutture dati di complessità arbitraria per managed object di SNMP. F**

    SMI permette l'utilizzo di un tipo limitato di sintassi.

69. **Nel sottoalbero del MIB con origine *.1.3.6.1.4.1* qualsiasi ente può richiedere un ramo privato. V**

    Il sottoalbero 1.3.6.1.4.1 è dedicato ai moduli specifici richiesti da enti privati, ovvero non ISO.

70. **Si definisce *agent* qualsiasi dispositivo fisico connesso in rete che supporti il protocollo SNMP. F**

    Anche i manager supportano il protocollo SNMP. Di conseguenza esistono dispositivi fisici che supportano SNMP senza essere agent.

71. **SNMP è un protocollo applicativo trasportato su UDP. V**

    In particolare gli agent sono in ascolto sulla porta 161.

72. **SNMP è utilizzabile per il monitoraggio di dispositivi, ma è principalmente impiegato per la loro configurazione. F**

Per la configurazione persistente sono ancora inevitabili strumenti proprietari, SNMP non si presta allo scopo. Viene invece usato per il monitoraggio di base.

73. **Solo la versione 3 di SNMP prevede sistemi di sicurezza robusti. V**
    SNMP v3 introduce l'user-based security model, che prevede l'autenticazione su un canale cifrato.
74. **In SNMP l'interazione tra manager e agent è sempre del tipo richiesta-risposta. F**
    L'agent può contattare il manager di sua iniziativa.
75. **Il MIB teoricamente è un modello per collocare in una tassonomia qualsiasi tipo di informazione. V**
    Il MIB è di fatto un catalogo che associa a ogni oggetto un OID, una sintassi e una codifica.

Configurazione centralizzata

76. **I tipi di attributo fondamentali per l'organizzazione delle entry LDAP per l'autenticazione sono *dc*, *ou*, *cn*, *uid*. V**
    In particolare dc è il domain component, ou è l'organizational unit, cn è il common name e uid lo user id.
77. **Il modello multimaster consente modifiche simultanee dello stesso database LDAP su diversi server. V**
    È il modello master-replica in cui le informazioni sono aggiornate periodicamente.
78. **LDAP è essenzialmente un database specializzato per distribuire informazioni relative a utenti. V**
79. **LDAP utilizza un modello relazionale dei dati. F**
    LDAP usa un modello gerarchico.
80. **Le entry LDAP possono essere trovate solamente conoscendo il loro Distinguished Name. F**
    Le entry LDAP possono essere trovate anche conoscendo un base DN, ovvero il punto del DIT da cui iniziare la ricerca, uno scope che indichi quanto estendere la ricerca, ed eventualmente un filtro.
81. **Una Object Class non è altro che la specifica di quali tipi di attributo siano necessari o ammessi in una entry che la istanzia. V**
82. **Il Distinguished Name identifica una entry LDAP ma non la sua posizione nel DIT. F**
    Il Distinguished Name identifica univocamente una entry LDAP all'interno del DIT, e intrinsecamente la sua posizione.

83. Le entry di LDAP possono essere mostrate secondo differenti organizzazioni gerarchiche. F

All'interno del DIT è presente una sola gerarchia.

84. Gli attributi di una entry LDAP sono come variabili a cui viene assegnato un singolo valore. F

Gli attributi LDAP sono simili alle variabili, ma presentano molti più vincoli: il singolo valore è solo uno dei possibili vincoli.

85. LDAP è un sistema autonomo che fornisce tutti i componenti necessari per l'autenticazione centralizzata di utenti. F

LDAP permette la configurazione centralizzata, e lo fa come una sorta di database che rappresenta la struttura interna di un ente in cui sono presenti gli utenti e i dispositivi, in modo tale da poterli configurare in un unico luogo senza modificare centinaia di macchine contemporaneamente.

86. Una entry LDAP può essere istanza di più classi simultaneamente. V

LDAP permette una sorta di ereditarietà multipla.